This is probably legit: WIKILEAKS GUY TRYING TO GET THROUGH. I FINALLY FIGURED OUT WHAT IS GOING ON

There has been a guy messaging me saying "the blockchain is compromised". I assumed Bitcoin, but now I know it is **Julian assanges dead man switch blockchain, for the huge releases he said he'd do if anything happened. This would obviously confirm he's in trouble because he is not here to correct the breaches. Here are a few of the messages sent:**

"Here are the tools to get Assange's information out of the blockchain. We are about to get gagged. Or worse. Pls do the right thing. These tools won't be around for long. FULL DISCLOSURE, let the people have the truth. No matter how damming. Sir, this information is dangerous. They killed Jean, and group one is missing. We need this public asap. We need more people involved. Be safe, sir. Thank you for being a true patriot. The tools will be improved if we can.https://github.com/WikiLeaksFreedomForce. And here is the bot link to the archived conversation as we built this. You will need the conversation to understand what to do. https://blargbot.xyz/logs/#3cvppr this is time sensitive. Thank you."

"I hope that if you have the resources available, you have people looking into the blockchain. The massive ddos was 10/21. We have found things, and others have reported finding full files and keys. We are working on discord in the open. Members of my team have gotten gag orders, and I'm sure my time is coming soon. Pls don't let this be for nothing"

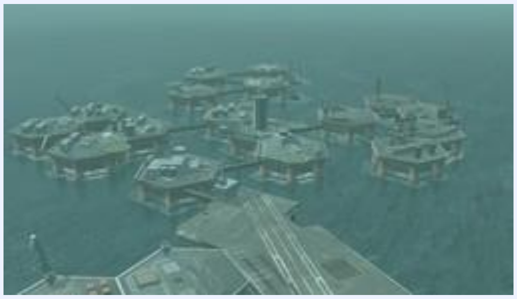
Also. We are unsure of if the blockchain was altered on Oct 27 2016. We have been using a local for our tests. U can find it on the darkweb. These tools... They are not perfected, but if u get your people on them. It will be more then enough to get you to the files. We still haven't combined the torrent magnets. And transmission of enclosed data seems to get people vanned. There has been multiple attempts to make this public for the past two months. Now, we have so many people doing this, I don't know if it can be stopped without shutting down the internet. This is what alot of people died for Jim. We're giving it to u first. And we will continue to share it with anyone interested. These kid fucking old guard types need to meet justice. And Julian deserves a legacy after this. The fact that his dms triggered indicates terrible things. My name is A___ K_____s. I live in Canada. I'm not the one who made this, I only helped. I'm not a spook. Nor a terrorist. Just a person who has had enough of the bullshit"

"Here are the tools to get Assange's information out of the blockchain. We are about to get gagged. Or worse. Pls do the right thing. These tools won't be around for long. FULL DISCLOSURE, let the people have the truth. No matter how damming. Sir, this information is dangerous. They killed Jean, and group one is missing. We need this public asap. We need more people involved. Be safe, sir. Thank you for being a true patriot. The tools will be improved if we can.https://github.com/WikiLeaksFreedomForce. And here is

the bot link to the archived conversation as we built this. You will need the conversation to understand what to do. https://blargbot.xyz/logs/#3cvppr this is time sensitive. Thank you."

http://82.221.129.208/baasepageh2.html

(202.19 KB 1440x816 438498967.jpg)



☐ **OUTER HEAVEN** Anonymous 12/07/2016 (Wed) 19:31:30 [Preview] No. 15 [X]

SALTS:
insurance.aes256 DE 18 1B 73 EF F3 5E 39 DA
wlinsurance-20130815-A.aes256 0F 0B DA 00 F0 35 9A 0F C8
wlinsurance-20130815-B.aes256 AB C2 04 75 6B AB 85 BE 30
wlinsurance-20130815-C.aes256 73 6B 46 4C 2F 84 9A C2 A4

INSURANCE SNIPPETS:
http://gateway.glop.me/ipfs/QmUUiWf1KLshZBQWHDt8yVaabHdMjJA2g1md7YS8qsvMci/insurance.aes256.5120
http://gateway.glop.me/ipfs/QmZHmQrNuBL1MJEi3cSn7bYoLShLiqGue5oeqZmcvHtBD6/wlinsurance-20130815-A.aes256.5120
http://gateway.glop.me/ipfs/QmRRAnoHgZGqMrJodHA3Nj6GeQ5j4y1AHUbG8MgVXWshMH/wlinsurance-20130815-B.aes256.5120
http://gateway.glop.me/ipfs/QmPCPmGwyCghyMrVENUB1AEbzkZ9dULE9rBJcVMqc5RG1M/wlinsurance-20130815-C.aes256.5120
http://gateway.glop.me/ipfs/QmNdwpvqWXkYsxPnjoL8rSZZpVDRDNu3YYvddsQ7dLdrEC/2016-06-03_insurance.aes256.5120
http://gateway.glop.me/ipfs/QmcDMXxr99Fi583oZKYqFzg8TwomugeV49oFkMrtGHEJ6Z/2016-11-07_WL-Insurance_EC.aes256.5120
http://gateway.glop.me/ipfs/QmPAoxkRcJERJEyj3uXsnKwe819WkqnX2Gp1VgpoaxLtys/2016-11-07_WL-Insurance_UK.aes256.5120
http://gateway.glop.me/ipfs/QmaYUUco1VtVurovbrtboMvu6kvFp9pdz6CEA97ftxojy5/2016-11-07_WL-Insurance_US.aes256.5120

FILES:
https://file.wikileaks.org/torrent/2016-11-07_WL-Insurance_US.aes256.torrent
https://file.wikileaks.org/torrent/2016-11-07_WL-Insurance_UK.aes256.torrent
https://file.wikileaks.org/torrent/2016-11-07_WL-Insurance_UK.aes256.torrent
https://file.wikileaks.org/torrent/2016-06-03_insurance.aes256.torrent
https://file.wikileaks.org/torrent/wikileaks-insurance-20120222.tar.bz2.aes.torrent
https://file.wikileaks.org/torrent/wlinsurance-20130815-A.aes256.torrent
https://file.wikileaks.org/torrent/wlinsurance-20130815-B.aes256.torrent
https://file.wikileaks.org/torrent/wlinsurance-20130815-C.aes256.torrent
https://web.archive.org/web/20100901162556/https://leakmirror.wikileaks.org/file/straw-glass-and-bottle/insurance.aes256

US Kerry [1]- 4bb96075acadc3d80b5ac872874c3037a386f4f595fe99e687439aabd0219809
UK FCO [2]- f33a6de5c627e3270ed3e02f62cd0c857467a780cf6123d2172d80d02a072f74
EC [3]- eae5c9b064ed649ba468f0800abf8b56ae5cfe355b93b1ce90a1b92a48a9ab72

sha256sum 2016-11-07_WL-Insurance_US.aes256 ab786b76a195cacde2d94506ca512ee950340f1404244312778144f67d4c8002
sha256sum 2016-11-07_WL-Insurance_UK.aes256 655821253135f8eabff54ec62c7f243a27d1d0b7037dc210f59267c43279a340
sha256sum 2016-11-07_WL-Insurance_EC.aes256 b231ccef70338a857e48984f0fd73ea920eff70ab6b593548b0adcbd1423b995

wlinsurance-20130815-A.aes256 [5],[6]
6688fffa9b39320e11b941f0004a3a76d49c7fb52434dab4d7d881dc2a2d7e02

wlinsurance-20130815-B.aes256 [5], [7]
3dcf2dda8fb24559935919fab9e5d7906c3b28476ffa0c5bb9c1d30fcb56e7a4

wlinsurance-20130815-C.aes256 [5], [8]
913a6ff8eca2b20d9d2aab594186346b6089c0fb9db12f64413643a8acadcfe3

insurance.aes256 [9], [10]
cce54d3a8af370213d23fcbfe8cddc8619a0734c

[1] https://twitter.com/wikileaks/status/787777344740163584
[2] https://twitter.com/wikileaks/status/787781046519693316
[3] https://twitter.com/wikileaks/status/787781519951720449
[4] https://twitter.com/wikileaks/status/796085225394536448?lang=en
[5] https://wiki.installgentoo.com/index.php/Wiki_Backups
[6] https://file.wikileaks.org/torrent/wlinsurance-20130815-A.aes256.torrent
[7] https://file.wikileaks.org/torrent/wlinsurance-20130815-B.aes256.torrent
[8] https://file.wikileaks.org/torrent/wlinsurance-20130815-C.aes256.torrent
[9] https://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010
[10] https://web.archive.org/web/20100901162556/https://leakmirror.wikileaks.org/file/straw-glass-and-bottle/insurance.aes256

☐ Anonymous 12/07/2016 (Wed) 19:33:27 [Preview] No. 16 [X] del

(49.57 KB 1113x651 1480438212028.jpg)

THREADS:
oniichanylo2tsi4.onion/thread-5b30554cf29073d3aee1a74c298234c8e36a7bad.html
https://oxwugzccvk3dk6tj.onion.to/tech/res/679042.html
https://s6424n4x4bsmqs27.onion.to/pol/res/20366.html
https://web.archive.org/web/20161030073742/http://8ch.net/pol/res/7946506.html
https://web.archive.org/web/20161023211637/https://oxwugzccvk3dk6tj.onion.to/pol/res/7931897.html
https://web.archive.org/web/20161024220236/http://8ch.net/pol/res/7962287.html
https://oxwugzccvk3dk6tj.onion.to/pol/res/8180723.html
https://oxwugzccvk3dk6tj.onion.to/tech/res/679042.html

DECODING ONE TX:
Download http://gateway.glop.me/ipfs/QmSU67Ei3TerNe32CcZTgd48jKqsVvBTgera1qBWFjKK9V/jean.py
(or http://gateway.glop.me/ipfs/QmburFHeUtM3wdrEj3rmUuBkx6iDmYpreyGCvHijgJhZnh/jean_b.py)
Usage:
```
python jean.py transaction_number
```

Example:
```
python jean.py 691dd277dc0e90a462a3d652a1171686de49cf19067cd33c7df0392833fb986a
```

Returns:
```
"Wikileaks Cablegate Backup

cablegate-201012041811.7z

Download the following transactions with Satoshi Nakamoto's download tool which can be found in transaction
6c53cd987119ef797d5adccd76241247988a0a5ef783572a9972e7371c5fb0cc Free speech and free enterprise! Thank you Satoshi!"
```

DECODING FILES:
A nice example is the original Bitcoin paper. It can be found in transaction

54e48e5f5c656b26c3bca14a8c95aa583d07ebe84dde3b7dd4a78f4e4186e713.

```
python jean.py 54e48e5f5c656b26c3bca14a8c95aa583d07ebe84dde3b7dd4a78f4e4186e713 > paper.pdf
```

Once it is done you will be able to see a pdf was generated in that directory.

Note that the transaction that generates the Bitcoin paper is related to the transaction that describes the Wikileaks cable dump, the cable dump itself, and many other transactions that have other content. Some has yet to be completely decrypted. These transactions are all related because they have common addresses involved or the money resulting from the transaction was used.

For example, take a look at this
transaction: https://blockchain.info/tx/08654f9dc9d673b3527b48ad06ab1b199ad47b61fd54033af30c2ee975c588bd

If you do

```
python jean.py 08654f9dc9d673b3527b48ad06ab1b199ad47b61fd54033af30c2ee975c588bd
```

You will get a key that was leaked.

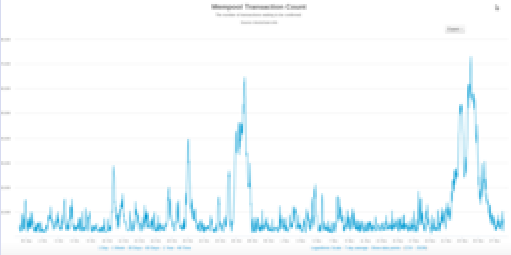
Now, if you look at the addresses involved, you can see one at the bottom, below Wikileaks. It does not show 'Escrow'. Go to that address and see its transactions. You will then find another message. Keep doing this and you'll eventually find the cable dump again. This is the process of 'following the change'.

Using this method we've found several transactions that involve Wikileaks that we don't quite understand. One good strategy is to generate a file from a transaction and then look at its 'magic numbers' to figure out what it could be.

Some of them are:
7379ab5047b143c0b6cfe5d8d79ad240b4b4f8cced55aa26f86d1d3d370c0d4c
d3c1cb2cdbf07c25e3c5f513de5ee36081a7c590e621f1f1eab62e8d4b50b635
cce82f3bde0537f82a55f3b8458cb50d632977f85c81dad3e1983a3348638f5c
2a14783f74796ace53e0a6859a7012723d3d6cd9dacf72d4e90a3394484093df
657aecafe66d729d2e2f6f325fcc4acb8501d8f02512d1f5042a36dd1bbd21d1
05e6c80d9d6469e7d1328e89b9d971b19972594701586bbcbd70070f2be799db
623463a2a8a949e0590ffe6b2fd3e4e1028b2b99c747e82e899da4485eb0b6be
5143cf232576ae53e8991ca389334563f14ea7a7c507a3e081fbef2538c84f6e

☐ Anonymous 12/07/2016 (Wed) 19:34:47 [Preview] No. 17 [X] del

(136.00 KB 1760x879 1480443142071.png)



>I might be compromised. So, before I get silenced, I'd like to present some tips for those investigating the blockchain angle (in the case that I am unable to continue my work):

>1. Sort transactions based on TX Fees. The DMS TX(s) will probably have a high fee associated with it to a) ensure its inclusion in the block (against the spamming attacks we're seeing) and b) draw attention to it. If a transaction contains an OP_RETURN and has an unusually high fee, IT IS WORTH INVESTIGATING.

>2. Look for duplicate OP_RETURN data. Provided there wasn't a lone machine setup to post the DMS, it would likely be posted twice or more. Create a script to store transactions in a database. Store block number, date, op_return, fee and amount (if any of the outputs contain "911", also pay attention.)

>3. The DMS will likely NOT come from the Wikileaks address (but might go to it). In the event that the server(s) hosting the DMS got compromised, the attacker would have access to that address' private key (and thus all of WikiLeaks' funds).

>4. This address might be worth investigating: htt ps://blockchain.info/address/1NquF1c4AuKx9YJtP9SsjGqhazfa72yPBM?offset=100&filter=0
Many OP_RETURNs and all on the 10/16/2016 within a period of a few hours. I have not had the chance to investigate further.

>Some side notes: Bootstrap8080.bitmessage.org and Bootstrap8444.bitmessage.org were down last night around 3AM (USA time). Worth checking DNS history on these to ensure they weren't compromised.

>My computer is sending ICMP packets routinely to addresses in San Francisco and UK. This is one of my reasons to suspect compromise (could these be packing non-erronous data?).

☐ Anonymous 12/07/2016 (Wed) 19:36:02 [Preview] No. 18 [X] del

(7.72 KB 704x480 1480988029588.jpg)

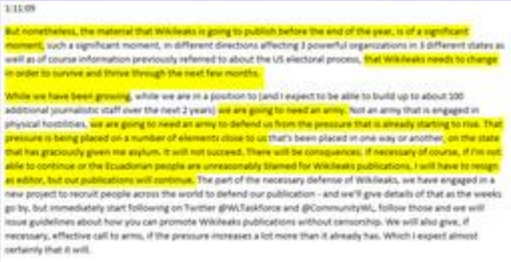
>Stop relying on scripts and crappy software. The steps to find every single file in the blockchain have been posted here numerous times >>22945. A lot of you have been staring at the data for over a week now. Here's another attempt at being even more clear:

>Every single file has a hex file header. You can see a list of some here: http://www.garykessler.net/library/file_sigs.html and here http://file-extension.net/seeker/seeker.cgi?ext=&filetype_AND=pgp&filetype_OR=&filetype_NOT=&seek=Seek%21 However, this is not the entire list. The lists 'trid' and 'file' use are not complete either. Yet, you don't even need these lists. You can simply look at any file of a type you are interested in finding. Yes, any. Open it with a hex editor and look at the file header. If you want to find a zip file, just download any zipfile, look at the header with a hex editor and then search for it. The headers are not going to always be at the beginning of the file. Scan the entire file for headers and footers.

>Yes footers. Files also have footers! You can find the ending of a file by looking for its hex footer. Here are some examples: http://www.datadoctor.biz/data_recovery_programming_book_chapter14-page2.html Again, this is not a complete list. If you want to see what the footer of a file looks like, open one with a hex editor.

☐ Anonymous 12/07/2016 (Wed) 19:37:08 [Preview] No. 19 [X] del

(454.10 KB 750x382 90375bb35550eb7e12a2e66070388123-imagejpeg.jpg)



1:11:09

But nonetheless, the material that Wikileaks is going to publish before the end of the year, is of a significant moment, such a significant moment, in different directions affecting 3 powerful organizations in 3 different states as well as of course information previously referred to about the US electoral process, that Wikileaks needs to change in order to survive and thrive through the next few months.

While we have been growing, while we are in a position to (and I expect to be able to build up to about 100 additional journalistic staff over the next 2 years) we are going to need an army. Not an army that is engaged in physical hostilities, we are going to need an army to defend us from the pressure that is already starting to rise. That pressure is being placed on a number of elements close to us that's been placed in one way or another, on the state that has graciously given me asylum. It will not succeed. There will be consequences. If necessary of course, if I'm not able to continue or the Ecuadorian people are unreasonably blamed for Wikileaks publications, I will have to resign as editor, but our publications will continue. The part of the necessary defense of Wikileaks, we have engaged in a new project to recruit people across the world to defend our publication - and we'll give details of that as the weeks go by, but immediately start following on Twitter @WLTaskforce and @CommunityWL, follow those and we will issue guidelines about how you can promote Wikileaks publications without censorship. We will also give, if necessary, effective call to arms, if the pressure increases a lot more than it already has. Which I expect almost certainly that it will.

For publishers for example, so that, as an example we are starting to use Bitcoin, Wikileaks, stuffing our, cryptographic keys of stuff that we publish, so, we prove that we have published stuff at a particular time by stuffing it in Bitcoin, in the blockchain, and then, if someone were to come and try to modify the material that we have published, to take a particular part, that would be detectable'. -Julian Assange, Nantucket Project, Sept 28 2104

Wikileaks needs to change in order to survive and thrive through the next few months... If necessary of course, if I'm not able to continue or the Ecuadorian people are unreasonably blamed for Wikileaks' publications, I will have to resign as editor, but our publications will continue. The part of the necessary defense of Wikileaks, we have engaged in a new project to recruit people across the world to defend our publication - and we'll give details of that as the weeks go by... ...we will issue guidelines about how you can promote Wikileaks publications without censorship. - Julian Assange, Wikileaks 10 Years Press Conference, Oct 4th 2016

☐ Anonymous 12/07/2016 (Wed) 19:38:20 [Preview] No. 20 [X] del

(38.06 KB 657x288 1480439159461.jpg)

https://en.m.wikipedia.org/wiki/Rubberhose_%28file_system%29
>The project was originally named Rubberhose, as it was designed to be resistant to attacks by people willing to use torture on those who knew the encryption keys. This is a reference to the rubber-hose cryptanalysis euphemism.
>It was written in 1997–2000 by Julian Assange, Suelette Dreyfus, and Ralf Weinmann.[

☐ Anonymous 12/07/2016 (Wed) 19:39:21 [Preview] No. 21 [X] del

(4.30 KB 213x236 1480440844495.jpg)

http://gateway.glop.me/ipfs/QmSYg1TfsV7yKW3hzQRy9qxMSDUgztka5vVu91S9sFVeuM/code-fixed.7z
To compile:

```
gcc bcrdr2.c sha256.c ripe160.c -lsqlite3 -o bcrdr2
```

To Run:

```
./bcrdr2 <blocks dir> <database file>
```

e.g:

```
./bcrdr2 ~/.bitcoin/blocks/ out.db
```

WHAT IT DOES:

This program reads through every file named blk*.dat in the folder to point it at and parses it.
It creates an sqlite3 database with the following schema:

```
CREATE TABLE BLOCK("
"ID INT PRIMARY KEY NOT NULL,"
"PREV CHAR(64) NOT NULL,"
"MERKLE CHAR(64) NOT NULL,"
"HASH CHAR(64) NOT NULL,"
"NUM INT ,"
"BITS INT NOT NULL,"
"NONCE INT NOT NULL,"
"TIME INT NOT NULL);";
```

Block header info, including the computed double SHA256 hash for the block.
PREV is previous block hash, MERKLE is the merkle root hash, HASH is this block's hash.
The other fields are miscellaneous.

```
"CREATE TABLE TX("
"ID INT PRIMARY KEY NOT NULL,"
"HASH CHAR(64) NOT NULL,"
"FILE TEXT NOT NULL,"
"OFFSET INT NOT NULL);";
```

Transaction header.
HASH is this transaction's SHA double hash.
FILE is the .DAT file's ID that it came from (See the FILE table below to get the file's name)
OFFSET is the offset in the file it came from.

☐ Anonymous 12/07/2016 (Wed) 19:41:19 [Preview] No. 22 [X] del

(132.20 KB 500x281 end .png)

(147.74 KB 500x281 end .png)

HOW TO GET THE KEYS (AND MORE) FROM THE BLOCKCHAIN:

The goal is to make very simple code that is easy to use and understand so that everyone can do this. This is a rough explanation of how it works.

There are two main approaches users are taking to decode messages in the blockchain. Scanning transactions, let's call this 'tx scanning', and scanning blocks, let's call this 'block scanning'. The main reason users are not yet able to see meaningful content is because both approaches have to be combined.

TX SCANNING:
When you scan by transactions, you look for a transaction number (tx id), and decode its contents. When you know the tx id, you can easily see which wallets were involved. Some messages require you to combine the decoded data from multiple tx ids. You can identify which tx ids are relevant by looking at transaction histories of the wallets involved. This strategy is used for the 'Cablegate Backup'. In that case, the list of tx ids is directly told to the readers in the first message. However, you can compile this list on your own by 'tx crawling'. To do this, follow these steps:
. For each tx, look at the wallets that received money and find those that spend it (in this case it is only one per tx).
. For that wallet, look at its transaction history and find a transaction that follows a similar pattern, i.e., it involves multiple wallets and only one spends the funds.
. Continue doing this until you are not able to see the pattern repeat itself.

BLOCK SCANNING:
When you scan by block, you will be able to find encoded data more easily but it is harder to extract the tx id and wallets. One benefit of block scanning is that you can explicitly search for file headers and important strings. For example you can directly search for the magic numbers in GPG files. When you find one of these, you can then tx crawl from that starting point in order to get all pieces of the file. More concretely, if you want to find the Cablegate Backup with a block scanner, you could search for the magic number of Zip files. Then, when one is found, you can find the tx id that contains it, and finally tx crawl to get all the pieces. Yet, file headers are just one of the many other patterns that can be used to find important transactions. Examples of others are:
. Magic numbers: Look for the first bytes in different types of file. 'file' can be used in UNIX.
. Ability to compress: Compress the decoded output. If the size is reduced, the output is possibly a message or part of a file.
. Text: If the decoded output has text, it might have information.
. Keywords (Very important): Search for relevant keywords, e.g., checksums for files in Wikileaks.org, checksums for the insurance files, hashes, dates, names, time stamps, etc.
. Reversibility: Some messages are in reverse and need to be flipped. This should be tried both before and after decoding.

☐ Anonymous 12/07/2016 (Wed) 19:41:31 [Preview] No. 23 [X] del

(132.20 KB 500x281 end_.png)

Both scanners have to be used. The starting points for the searches should be Wikileak's wallet, important dates (for example, during the DDoS attacks), previous messages and checksum hashes. The Cablegate Backup was a bit simpler than the more recent messages. In that case, only one wallet spent the funds in each transaction, and simply looking at wallet's next transaction was enough to find all the pieces. Newer messages are bit more complicated. Some of the wallets that receive money make multiple transactions with no encoded data before proceeding with the 'real' transaction. Moreover, in a lot of cases, all wallets involved spend the funds (not just one). Therefore, the crawler has to keep track of all wallets that receive funds, and all future transactions of that wallet while using techniques (like those above) to detect encoded data. A transaction tree should be kept and the pieces of each files should be combined in multiple orderings.

If you implement the process described above you will find all the keys, other backups and other files that are not released. One way to test your code is to search for checksum hashes for files that have already been published at a specific date. There are multiple messages in the blockchain that include file hashes and dates. [/spoiler]Use the leads in this thread.[/spoiler]

I recommend you use a local copy of the blockchain and carry out the search on a computer that has no internet access. Work in groups and share the process. Remember to look at other cryptocurrencies as well and to encode your findings into the blockchain yourself.

Good luck!

☐ Anonymous 12/07/2016 (Wed) 19:43:02 [Preview] No. 24 [X] del

(1001.41 KB 500x212 contact.gif)

FAST POSTING:
Download Gajim https://gajim.org/ (or any Jabber client that supports OTR and a proxy option https://wikipedia.org/wiki/List_of_XMPP_client_software)
Download OTR plugin https://dev.gajim.org/gajim/gajim-plugins/wikis/OffTheRecordPlugin https://dev.gajim.org/gajim/gajim-plugins/tree/master/gotr(Or the plugin needed for your Jabber client)
Create a GPG key (if using GPG for encryption and not OTR)

Make account:
Server: volatile.ch
Advanced:
Hostname: vola7ileiax4ueow.onion Port: 5222
Make a new proxy option with manage to: 127.0.0.1 9050 (socks5)

Preferences (for volatile account):
Disable 'Allow client / OS information to be sent'
Disable 'Allow local system time information to be sent'
Disable 'Log encrypted chat session'
Disable 'Allow my idle time to be sent'

Edit > Accounts > General (for volatile account):
Disable 'Synchronize accounts status with global status'
Disable 'Save conversation logs for all contacts'

☐ Anonymous 12/07/2016 (Wed) 21:27:50 [Preview] No. 25 [X] del

join chat room "ebin" on muc.volatile.ch

☐ Anonymous 12/07/2016 (Wed) 22:20:15 [Preview] No. 26 [X] del

This is the new bunker. Old endchan thread compromised

☐ Anonymous 12/08/2016 (Thu) 18:35:18 [Preview] No. 27 [X] del

BLOCK 435250

Link Anomaly Status Amount Size Time
https://blockchain.info/tx/64abaf5ffac37f41c5a1b8b52deb5a21c7400b2a4e1f20433bb3120c6c36ae51 Unable to decode output address Unspent 0 288 2016-10-21 13:16:09
https://blockchain.info/tx/3410d6264a83683ce785289eebd17f7ccb14b7b2abcee34ece534cf1b75087c9 Unable to decode output address Unspent 0 269 2016-10-21 13:16:09

https://blockchain.info/tx/26a78bfda83f5f6b6bae3957ca1aca31519436617902ea74220233b868b2a805 Unable to decode output address Unspent 0 256 2016-10-21 13:16:09
https://blockchain.info/tx/6e412ca6112f0f0f14680d83151033ba18035eb4b81387f1f9ce38df3c6893af Unable to decode output address Unspent 0 242 2016-10-21 13:16:09
https://blockchain.info/tx/5fbfe2dbc0965cc1d74ecc06a1e4a776d4303a40c8f716168ab6ad01a87794ea Unable to decode output address Unspent 0 242 2016-10-21 13:16:09
https://blockchain.info/tx/a9dbcd57268b4b6d7eb40e09c5b5970f2c4d897bd3d47f83be658bfbc45580f1 Unable to decode output address Unspent 0 275 2016-10-21 13:16:09
https://blockchain.info/tx/17202c7ae9efec4dae73db145ea61de1fae090fd57d667f318871de45d799bc1 Unable to decode output address Unspent 0 275 2016-10-21 13:16:09
https://blockchain.info/tx/0fb02f09d710737cdd4c0d47c50774a7a11ae548b972f071965935955a1315b4 Unable to decode output address Unspent 0 648 2016-10-21 13:16:09
https://blockchain.info/tx/944de0e90a70ca656400f37d4b5de7619dd0874ad9a8c1709f500c54310ba2e7 Unable to decode output address Unspent 0 264 2016-10-21 13:16:09
https://blockchain.info/tx/0c8e715db1a79a8020e8f292c08f20749dfb8b59e5048884f82c22ac3293a9a6 Unable to decode output address Unspent 0 265 2016-10-21 13:16:09
https://blockchain.info/tx/11d40e3c6e11de924be7ec71af2d76cbdddd7a6359a6ea672787aca4ce25c5fb Unable to decode output address Unspent 0 237 2016-10-21 13:16:09
https://blockchain.info/tx/2cd710205c0249eea43d0e589a6beabc9a9d488fc0c9c8e2497b48dfbf9e0911 Unable to decode output address Unspent 0 237 2016-10-21 13:16:09
https://blockchain.info/tx/82e7daf19b24d4f3228d14a88add9f7b401951d82181ed532f739cf3c1fa2022 Unable to decode output address Unspent 0 237 2016-10-21 13:16:09
https://blockchain.info/tx/aa23347580cc98b47bd662ae418de250141f22b8649dcb79630e56bfc80ea445 Unable to decode output address Unspent 0 238 2016-10-21 13:16:09
https://blockchain.info/tx/d295f447d25a3c8969e110c9c6a34d92ad86eafa8083ee5dcd449acb369d287c Unable to decode output address Unspent 0 239 2016-10-21 13:16:09
https://blockchain.info/tx/6ecf2b6d21312584c51550534729589c195a4fe5970688384b3ea76477fd9afe Unable to decode output address Unspent 0 297 2016-10-21 13:16:09
https://blockchain.info/tx/a0711aad3475b773f408779aa5aecc523e2c213cecb0f7a93d7d46ff1c136e18 Unable to decode output address Unspent 0 296 2016-10-21 13:16:09
https://blockchain.info/tx/59d41ca2325c74439a84c2a7eb46033fe213315e9e187c16dc6a8cb702adffaf Unable to decode output address Unspent 0 296 2016-10-21 13:16:09
https://blockchain.info/tx/18f6ae5323aff1dca6cf4fc4157fff5a990b37f0e3e43f762e9df5cadce08982 Unable to decode output address Unspent 0 296 2016-10-21 13:16:09
https://blockchain.info/tx/884736546d806654781f4d145b87e9e947aaf0f76d28e3c4fa399fe2d89a5c43 Unable to decode output address Unspent 0 264 2016-10-21 13:16:09

☐ Anonymous 12/08/2016 (Thu) 18:38:48 [Preview] No. 28 [X] del

(74.61 KB 1068x671 screen.png)

☐ Anonymous 12/08/2016 (Thu) 18:40:46 [Preview] No. 29 [X] del >>30

https://blockchain.info/address/1L8WoLjjGjNyj3TXXW4nMZMwLpKZeV3gKf
https://blockchain.info/tx-index/185992996

☐ Anonymous 12/08/2016 (Thu) 18:42:26 [Preview] No. 30 [X] del

>>29
https://blockchain.info/tx/74f9fcb4e1d047278d46cbbba81331abcb2628ea9e250c9a960c002538c664d9

☐ Anonymous 12/08/2016 (Thu) 19:10:05 [Preview] No. 31 [X] del

NEW CODE:
https://github.com/WikiLeaksFreedomForce

☐ Anonymous 12/08/2016 (Thu) 19:38:11 [Preview] No. 32 [X] del

FILE ASSEMBLY CODE:
http://gateway.glop.me/ipfs/QmVWJVbis7es6s7cDsRmt5WBHeioc4HztR4R74Lg8KBmhU/e0911.php

☐ Anonymous 12/08/2016 (Thu) 19:46:48 [Preview] No. 33 [X] del

(21.25 KB 435205block.zip)

http://gateway.glop.me/ipfs/QmQnjYcDmRMoNCSkaNjwLaBZMFFT3yX8GmF25S9TdJfpRT/435205block.zip

☐ Anonymous 12/08/2016 (Thu) 20:04:21 [Preview] No. 34 [X] del

https://blockchain.info/address/135zDqhbNcmPk3gbyeJmH75yiLdVZechsK?offset=13350&filter=4

☐ Anonymous 12/08/2016 (Thu) 20:10:09 [Preview] No. 35 [X] del

https://blockchain.info/address/1E14k7i1wVSytoMfbaCnbmhofVMNsZrpLh

☐ Anonymous 12/08/2016 (Thu) 20:17:03 [Preview] No. 36 [X] del

(84.26 KB 1062x671 new.png)

https://blockchain.info/tx/624075b5d5d56b619b413966297b441ae727fc019871c22676405dd5d8200cc9
View information about a bitcoin transaction 624075b5d5d56b619b413966297b441ae727fc019871c22676405dd5d8200cc9
>OMG
>I thnk I found it
>hang on
>look at this
https://blockchain.info/block/0000000000000000026fb408f6a035e55c126a1409e9c5f5fea7d22610645289
>Transactions contained within bitcoin block 435172
>scroll down to roughly

>It's possible that a 7z or other compressed text document with instructions is hidden within a single transaction
>And that transaction is spent.

>37 7a bc af 27 1c 20 04 0e 15 c8 0f 26 20 20 20 20 20 20 20 62 20 20 20 20 20 20 20 50 c7 af >be 01 20 21 67 73 63 6c 69 6c 69 70 74 72 68 6e 65 74 65 65 74 73 67 68 69 6e 61 65 75 6f 64 >69 6e 65 72 72 69 69 20 01 04 06 20 01 09 26 20 07 0b 01 20 01 21 21 01 20 0c 22 20 08 0d 0a >01 86 66 4f f7 20 20 05 01 19 0c 20 20 20 20 20 20 20 20 20 20 20 20 11 17 20 77 20 6c 20 63 >20 6f 20 64 20 65 20 2e 20 74 20 78 20 74 20 20 20 19 04 20 20 20 20 14 0d 0a 01 20 bd 31 89 >c3 e9 42 d2 01 15 06 01 20 20 20 20 20

>That's a possible 7z encrypted message, albeit a small one

https://blockchain.info/address/1E14k7i1wVSytoMfbaCnbmhofVMNsZrpLh
Transactions sent and received from bitcoin address 1E14k7i1wVSytoMfbaCnbmhofVMNsZrpLh.
https://blockchain.info/tx/4aadbaa0edd0f0b19d5e8ae0a818e3ac7fde7cd5f6caedcd9cf4e7ac2b9582e9
View information about a bitcoin transaction 4aadbaa0edd0f0b19d5e8ae0a818e3ac7fde7cd5f6caedcd9cf4e7ac2b9582e9

☐ Anonymous 12/08/2016 (Thu) 20:37:42 [Preview] No. 37 [X] del >>39

1Gii1VoJksAKrL34Gd4sLF1bUTQdUq1qe1 and i dont know if this is old news but this should be JA's address.. There's a DMS at the beginning of the txs
First being oldest. 1Fpdrx7Q7fVgf19imhXeDwNEhBAQV1a6Gp

for example this is one of the 4 txs.. its cryptic so "im dead when back" and likely implies something to do with the hex

If you look at the oldest tx on Gii, you'll see what looks like a dms.. Y is for key. It's always been here but it needs to be disarmed. Thats basically what it is.

The account basically returns what is sent to it.. which is what this 'QdUq1qe1'

The unconfirmed tx has actually been there since this weekend since I found it but it looks like it rejected it and has one from 12/6
http://gateway.glop.me/ipfs/QmXUMj6fRG9mNHLTgythygDJxUodGCnWFkBfcQfaqZo896/outtx.xlsx

list of unable to decode from block 435251
435251.xlsx
list of unable to decode from block 435252
435252.xlsx
http://gateway.glop.me/ipfs/QmTtdJr3sEYeWSHdgWTyP7uq89YRQWyUKbyWYcbeBKY6kh/435251.xlsx
http://gateway.glop.me/ipfs/QmUs1xK7wf89gf9t4wtdRNPpVdaQgnsmLDBcuBrbFcQT5v/435252.xlsx
http://gateway.glop.me/ipfs/QmUttF4q2JgjzGgKkuJoXvWvUaVZvG47XKAguHDYRX1NXP/block_435250_unable_to_decode.xlsx

There's only one that had any actual value associated (it's on the list ending in 51) all other transactions have shown as 0

an example would be if you find a hex code for a 7zip header
such as in https://blockchain.info/tx/5c593b7b71063a01f4128c98e36fb407b00a87454e67b39ad5f8820ebc1b2ad5
View information about a bitcoin transaction 5c593b7b71063a01f4128c98e36fb407b00a87454e67b39ad5f8820ebc1b2ad5
at bottom 377ABCAF271C
that is the hex code for a 7zip header
also i believe this has footer http://www.7-zip.org/recover.html

just to make sure im not wasting my time, is it a waste of time to be looking at https://blockchain.info/address/135zDqhbNcmPk3gbyeJmH75yiLdVZechsK?offset=10800&filter=4, batches of transactions ~20 each(sometimes significantly more such as the 57 on the 21) at same time. literally thousands of transactions in a row with same file size
throuugh 300 some odd pages, other than the first few, there are only 3 file sizes
and average bitcoin transaction is ~.001 over 84444 transactions

this one is huge...
https://blockchain.info/tx/842a17b3a797ec03c7ab856a6e62103c3288e03d790c8dc00a6e9175d164ece0

https://blockchain.info/address/135zDqhbNcmPk3gbyeJmH75yiLdVZechsK?offset=15250&filter=4
Transactions sent and received from bitcoin address 135zDqhbNcmPk3gbyeJmH75yiLdVZechsK.
same size transactions but changes size on oct 9
fucktons of transactions for weeks all of which are same size

https://blockchain.info/ip-address/47.89.39.165, a lot of same size same time transactions and unable to decode output

http://gateway.glop.me/ipfs/Qmaut7iGTaCoVZE4RAuV6cNBY5B2HxYgZDpaFrpKYKqYgH/Filenames_16D.txt
http://gateway.glop.me/ipfs/QmUUWrmeCQrhVQrbVBJqKKBbEWoHEpgWPoKhKi6Yune52Q/Filenames_16G.txt

☐ Anonymous 12/08/2016 (Thu) 20:55:23 [Preview] No. 38 [X] del

7b03d286ecb410884a5e07e41b6a7be1509afa99e4e001003f71bb319dfe84dd

e0f3a7f25bfb9415a116f26d7f718782157c3772f0e67acc00af2b8aa4309fb7

603c128766c75160b533f4f6cfbf1568c9ae7cb238a20791da7437c60afd814b

20aaf28f5030dcb5bcfe9d1d2ed632d213671ebef78587e3a629c7a3bdf0d93b

a2feacf1a3e2d1e2852326b26e67a22cb784a7c0d6f1d99213ee12b389188218

6e2bead2e61fd87f23e75ad29389f4e58db92b7a96c04e81f5133f29e50f52ac

d515d0eae9ea00fe16b9335ab946339d6eeef00c7f77c44c2ef41fab738f4401

da43c8be1c81ef20c93014341f7dcb744fff0388fcf6d214a84be4895fa2270b

this wallet

https://blockchain.info/address/1AfdbCzDrRrMEqAXkF8kxVRCkPzB8HxoHD?offset=400&filter=1

wtf?
must be either a wallet no one cares about or a bug like the wallet with the ripemd hash 0000000000000000000000

☐ Anonymous 12/08/2016 (Thu) 21:10:12 [Preview] No. 39 [X] del

>>37
https://blockchain.info/address/1Gii1VoJksAKrL34Gd4sLF1bUTQdUq1qe1

☐ Anonymous 12/08/2016 (Thu) 21:39:22 [Preview] No. 40 [X] del >>41

Possible tip:

https://blockchain.info/tx/7f1e4e76084ab2a44b484358900d74261e4629879db173b85251cb54cac21070
https://blockchain.info/address/1NAQExkFZTFJKQq76KoyUosoQEfiY8K9GN
https://blockchain.info/address/1B896LaaMVJvQD84ko52XN3976gaKA7nXJ

Multiple 'Escrows'. Seems like addresses are using the change as in cablegate.7z.

☐ Anonymous 12/08/2016 (Thu) 21:41:45 [Preview] No. 41 [X] del

>>40
From:
7141f6c62892c4c3b85aa989ba54b27be274f5200a715439a75d44b3331da30f
1883ec71f568cb0644606d2fbfd57e9b01d008503f90b6d934b56d548c08f33d
c9924669d668e2bcc6c64038f6a33c984cff3d8be758852911f8414666034046
56f5a921d6fe990715fef88b56379ba2716aa80ec02f4310fa47e2e68ae700e4
eb540314f01a8f79301b3b2fdd2f3dbf162f343b38b913cd860aae21a2a63f34
f19c51e46adb68e9235637d7b68d59e0bff6bc8cc0103c44214efcfe9aa140af
8e3b1e5d7a290d78b0e34fd54c97da3274c3d5a1549ff1228bdb63551fb11dc6
5501f5a1930640ee9e554a254d8df29a14b5f5fbc97c31aa0232f9a7202976c9
319ffa215f446d50091d6900c284319d3d95a0c21ff0ec5b77cf0c08ffc22d52
718c3be4557660259e38e041a04f7703e8ade3803ab79eda3bc700aeeca96628
bad344983f7bfa0f84f2befae1e178c55b90dbecb1aadc074643e159e34054f1
5fb72ef284c4bf131ffa57ba957d03e28e4e9e0ce53ceb6a97e84bab3d11fc1d
60d5d25c4c55a032e3842770495d72ff2f4f7c811a522a18e51b49e192132283
7bafcd844fc308280828d2685ab506bd88310653fe7cf43d380cb21a333bf9d1
69ac8f52cdad01aa7f5d97ff8903a536e52d43026dfac98dabb1ffac9343808b
4218dacb23d2a9a09843e11e1f0c1c467ff0640c381c3022b34309d847c73584

☐ Anonymous 12/08/2016 (Thu) 22:00:46 [Preview] No. 42 [X] del

(5.33 KB list.txt)

all from 435165-435382 (some are missing because API limits), spent < 33%, avg unspent value < 0.001 btc, at least 4 outputs
https://codepaste.net/ta5hyb

☐ Anonymous 12/09/2016 (Fri) 01:07:12 [Preview] No. 43 [X] del

(2.45 MB txs.txt)

spent < 51%, avg unspent value < 1btc, at least 2 outputs

☐ Anonymous 12/09/2016 (Fri) 04:16:55 [Preview] No. 44 [X] del >>61

does anyone have a backup of the endchan thread with the posts of the 7z footer and the screenshot of the deleted files from wikileaks.org?

☐ Anonymous 12/09/2016 (Fri) 04:32:15 [Preview] No. 45 [X] del >>55>>61

https://archive.fo/46rS9

☐ Anonymous 12/09/2016 (Fri) 05:32:08 [Preview] No. 46 [X] del

Discord #blockchain log bot for past two days

https://blargbot.xyz/logs/#3cvppr

☐ Anonymous 12/09/2016 (Fri) 06:20:27 [Preview] No. 47 [X] del

(812.71 KB 1145x1600 blockchain.png)

☐ Anonymous 12/09/2016 (Fri) 06:31:19 [Preview] No. 48 [X] del >>55>>61

(165.70 KB 960x540 Screenshot_20161208-223040.png)

☐ Anonymous 12/09/2016 (Fri) 06:34:54 [Preview] No. 49 [X] del >>61

That last one is one of the missing posts from here I think. Headers/footers. Run off local. Please share the pictures above after confirming for yourselves.

☐ Anonymous 12/09/2016 (Fri) 15:28:18 [Preview] No. 50 [X] del

https://github.com/manly/BlockChainParser

☐ Anonymous 12/09/2016 (Fri) 15:30:10 [Preview] No. 51 [X] del

https://m.box.com/shared_item/https%3A%2F%2Fapp.box.com%2Fs%2Fkiqg2ri8igt70i87av0sy3wq3i1zcro7

☐ Anonymous 12/09/2016 (Fri) 15:32:42 [Preview] No. 52 [X] del

We are working hard. Come check in at discord. Let's get this done. The more people on this, the more impossible will be to stop. Let's not let Jean be forgotten. https://discord.gg/3eV4N

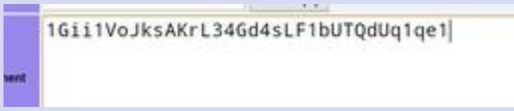
☐ **Possible dms wallet?** Anonymous 12/09/2016 (Fri) 16:06:40 [Preview] No. 53 [X] del

1Gii1VoJksAKrL34Gd4sLF1bUTQdUq1qe1

Have not linked to JA/wl personally, could someone take a look at this thing?? Definitely something weird here

☐ Anonymous 12/09/2016 (Fri) 16:09:25 [Preview] No. 54 [X] del

(10.97 KB 540x107 IMG_20161209_080758.jpg)



1Gii1VoJksAKrL34Gd4sLF1bUTQdUq1qe1

1Gii1VoJksAKrL34Gd4sLF1bUTQdUq1qe1 reposting screen shot.... The first post is glitching the last seven characters on my end?

☐ Anonymous 12/09/2016 (Fri) 17:09:24 [Preview] No. 55 [X] del >>61

>>48
>>45
the last post was a screenshot of wikileaks.org showing how some files were deleted

☐ Anonymous 12/09/2016 (Fri) 19:05:56 [Preview] No. 56 [X] del

sample .FLI videos. this format is commonly used for maps like
this https://woodshole.er.usgs.gov/operations/modeling/circulation.html they come out of cad software like autodesk
http://gateway.glop.me/ipfs/QmTUHgamFyoUwesutXosfGprHYMn2ywX6MGp3ryYKDxDjQ/2ARMS.FLI
http://gateway.glop.me/ipfs/QmTvByE3pVGpnsg2eayY1kmxHfguXDjxC5nZfvxz3hWyL4/APACHE.FLI
http://gateway.glop.me/ipfs/QmV2jhMzqdr3S35YCrukhhAC1KnKKQ36UYGSXM7Zs9H9J2/BUGS.FLI
http://gateway.glop.me/ipfs/QmdxjHSGTZkuvj6gaPmXWDDLCjxbqbEjY5ZZbamBRUQ8DT/MANTA.FLI
http://gateway.glop.me/ipfs/Qmd8oTT3YsYRswxWxAfaGWdZNyxG1pcEAKMe8fCLaNa8JK/MSH.FLI

☐ Anonymous 12/09/2016 (Fri) 19:16:07 [Preview] No. 57 [X] del

HOW TO SPLIT AND UPLOAD GIANT FILES:
1. Take giant file and slip it into pieces with 7zip
Linux: http://superuser.com/questions/184557/how-to-create-multipart-7zip-file-in-linux
Example:
7z -v100m a my_zip.7z my_folder/
Windows: http://www.linglom.com/it-support/how-to-split-a-large-file-using-7-zip/
2. Upload the pieces to mega.nz or filedropper (max 5GB):
filedropper.com
mega.nz
2b (optional). Do it from the command line to save time:
https://megatools.megous.com/
Example:
https://youtube.com/watch?v=LWfFMysaspQ [Embed]&feature=youtu.be

FILES WE NEED UPLOADS FOR:
1. All insurance files
2. Blockchain
3. SQL databases of the blockchain
4. wikileaks.org

☐ Anonymous 12/09/2016 (Fri) 19:37:02 [Preview] No. 58 [X] del

j0dumpprivkey <31qneokFGwpEkoZRksjymxZAiTEmAim3Ab>

☐ Anonymous 12/09/2016 (Fri) 19:52:38 [Preview] No. 59 [X] del

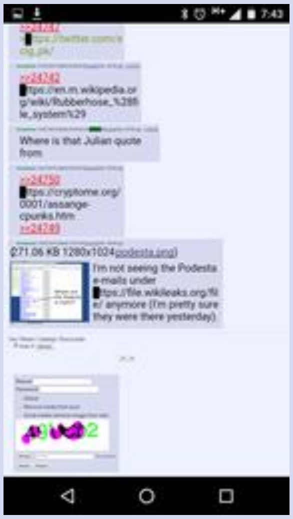
If the internet goes down soon:

https://www.geckoandfly.com/22562/chat-without-internet-connection-mesh-network/

http://www.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/
http://hyperboria.net/

☐ Anonymous 12/09/2016 (Fri) 19:57:06 [Preview] No. 60 [X] del >>61

(120.13 KB 540x960 end.png)



7:43

>>24742
[redacted]ttps://en.m.wikipedia.org/wiki/Rubberhose_%28file_system%29

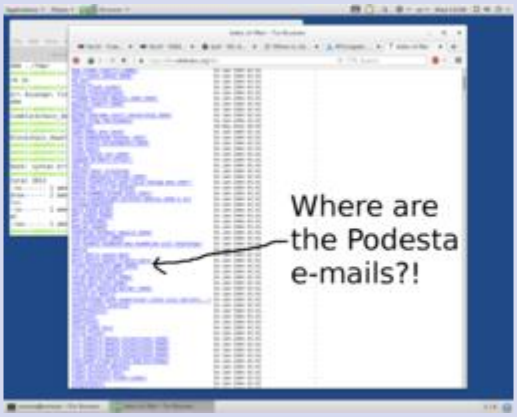
Where is that Julian quote from

>>24750
[redacted]ttps://cryptome.org/0001/assange-cpunks.htm
>>24749

(271.06 KB 1280x1024 podesta.png)
I'm not seeing the Podesta e-mails under [redacted]ttps://file.wikileaks.org/file/ anymore (I'm pretty sure they were there yesterday)

☐ Anonymous 12/09/2016 (Fri) 20:07:40 [Preview] No. 61 [X] del

(271.06 KB 1280x1024 endend.png)



Where are the Podesta e-mails?!

>>60
>>55
>>49
>>48
>>45
>>44

☐ Anonymous 12/09/2016 (Fri) 21:17:37 [Preview] No. 62 [X] del

(30.92 MB EndChanPOL_Thread.zip)

full bread

☐ Anonymous 12/09/2016 (Fri) 21:49:11 [Preview] No. 63 [X] del >>66

thanx

☐ Anonymous 12/09/2016 (Fri) 21:53:01 [Preview] No. 64 [X] del

podesta emails file was gone and up again some time later

☐ Anonymous 12/09/2016 (Fri) 22:06:52 [Preview] No. 65 [X] del

(821.28 KB 183x255 wew.gif)

EXTREMELY RARE LIMITED EDITION MISPRINT PEPE
WARNING: THIS EXTREMELY RARE PEPE HAS ONLY 1 KNOWN COPY. DUPLICATION BY SAVING AND DISTRIBUTING IS STRICTLY PROHIBITED AND PUNISHABLE BY UP TO 25 YEARS IN FEDERAL PRISON WITH A FINE UP TO $10,000,000.
1ST EDITION
V.1

PROTIP:
Download first insurance file: https://web.archive.org/web/20100901162556/https://leakmirror.wikileaks.org/file/straw-glass-and-bottle/insurance.aes256
Write a python script that tries words from a dictionary on it and writes down the ones that don't have errors (example ONION). (make sure to try with different both lower and upper case)
Read words that don't produce errors.
[redacted]

☐ Anonymous 12/09/2016 (Fri) 22:07:48 [Preview] No. 66 [X] del

>>63
did you diff them after? might want to...

☐ Anonymous 12/10/2016 (Sat) 00:02:37 [Preview] No. 67 [X] del

https://i.imgur.com/nTYDpPb.png

☐ Anonymous 12/10/2016 (Sat) 02:24:56 [Preview] No. 68 [X] del >>69

most are not verified

headers:
doc D0 CF 11 E0 A1 B1 1A E1
xls D0 CF 11 E0 A1 B1 1A E1
ppt D0 CF 11 E0 A1 B1 1A E1
zip 50 4B 03 04 14 (I think this one is wrong)
jpg FF D8 FF E0 00 10 4A 46 49 46 00 01 01
gif 47 49 46 38 39 61 4E 01 53 00 C4
pdf 25 50 44 46 2D 31 2E (I think this one is wrong too)
7zip 37 7A BC AF 27 1C (verified at endchan)
Torrent 64 38 3A 61 6E 6E 6F 75 6E 63 65
AVI 52 49 46 46

footers:
doc 57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E
xls FE FF FF FF 00 00 00 00 00 00 00 00 57 00 6F 00 72 00 6B 00 62 00 6F 00 6F 00 6B 00
ppt 50 00 6F 00 77 00 65 00 72 00 50 00 6F 00 69 00 6E 00 74 00 20 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74
zip 50 4B 05 06 00 (probably wrong)
gif 21 00 00 3B 00
pdf 25 25 45 4F 46 (probably wrong)
7zip 00 00 00 17 06 (verified with cablegate)

we are waiting for someone to post the headers and footers for all pgp, gpg files. they can be found by searching for common hex blocks in different files of the same type. someone finished this list but has not posted it. hopefully it's up today.

☐ Anonymous 12/10/2016 (Sat) 04:51:03 [Preview] No. 69 [X] del

>>68
I used a batch with GPG on bash for an 8192 key

```
Key-Type: RSA
Key-Length: 8192
Name-Real: Name
Name-Email: name@email.com
Expire-Date: 10y
Preferences: SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES TWOFISH CAST5 BZIP2 ZLIB ZIP Uncompressed
```

That let me create an 8192 key.

and Thanks for the input!

PGP 2048 PUBLIC KEY HEADER
mQENBFhLe

PGP 4096 PUBLIC KEY HEADER
mQINBFhLe

PGP 2048 KEY PAIR HEADER
.XK (with this there was suble variety before the string to the left, either >, 1/2, or 3/4 before the ".") for example, these are the strings in three test files:
1: •.½.XKz
2: •.>.XK{
3: •.¾.XK|

PGP 4096 KEY PAIR HEADER
•.>.XKz (this was consistent across 2 test files)

PGP 4096 PRIVATE(SECRET) KEY HEADER
•.>.XKz

PGP 2048 PRIVATE KEY HEADER
similar results to the key pair, three files. 2048 may have something different going on than 4096.
1: •.½.XK
2: •.>.XK
3: •.¾.XK

PGP 4096 PRIVATE KEY HEADER
•.>.XKz

8192 isn't supported by kleo generation so i'm lookin for a way to do that, if someone else can chip in i'd apprecaite it.

Hope this helps.

Yes, outside the BEGIN PUBLIC/PRIVATE KEY part. You don't need to convert it to hex I can do that but it would help doccumenting it like the previous magic numbers posted. 2048, 4096, and 8192 keys are what I want to search for.

I presume you mean outside of the -------BEGIN PUBLIC PGP KEY------ etc. strings right?

☐ Anonymous 12/10/2016 (Sat) 07:05:38 [Preview] No. 70 [X] del

There news that some groups are starting to find torrent headers in the blockchain. Some advice regarding that.

1. Check the file structure.
A torrent file is a bencoded dictionary with the following keys:
announce—the URL of the tracker
info—this maps to a dictionary whose keys are dependent on whether one or more files are being shared:
name—suggested filename where the file is to be saved (if one file)/suggested directory name where the files are to be saved (if multiple files)
piece length—number of bytes per piece. This is commonly 28 KiB = 256 KiB = 262,144 B.
pieces—a hash list, i.e., a concatenation of each piece's SHA-1 hash. As SHA-1 returns a 160-bit hash, pieces will be a string whose length is a multiple of 160-bits. If the torrent contains multiple files, the pieces are formed by concatenating the files in the order they appear in the files dictionary (i.e. all pieces in the torrent are the full piece length except for the last piece, which may be shorter).
length—size of the file in bytes (only when one file is being shared)
files—a list of dictionaries each corresponding to a file (only when multiple files are being shared). Each dictionary has the following keys:
path—a list of strings corresponding to subdirectory names, the last of which is the actual file name
length—size of the file in bytes.
2. Check the tracker information.
Multiple trackers
BEP-0012[4] extends BitTorrent to support multiple trackers.
A new key, announce-list, is placed in the top-most dictionary (i.e. with announce and info)
{
...

```
'announce-list': [['<tracker1-url>']['<tracker2-url>']]
...
}
```

3. If it a single file or Multi file torrent

Single file[edit]
Here is what a de-bencoded torrent file (with piece length 256 KiB = 262144 bytes) for a file debian-503-amd64-CD-1.iso (whose size is 678 301 696 bytes) might look like:

```
{
'announce': 'http://bttracker.debian.org:6969/announce‘,
'info':
{
'name': 'debian-503-amd64-CD-1.iso',
'piece length': 262144,
'length': 678301696,
'pieces': '841ae846bc5b6d7bd6e9aa3dd9e551559c82abc1...d14f1631d776008f83772ee170c42411618190a4'
}
}

{
'announce': 'http://tracker.site1.com/announce‘,
'info':
{
'name': 'directoryName',
'piece length': 262144,
'files':
[
{'path': ['111.txt'], 'length': 111},
{'path': ['222.txt'], 'length': 222}
],
'pieces': '6a8af7eda90ba9f851831073c48ea6b7b7e9feeb...8a43d9d965a47f75488d3fb47d2c586337a20b9f'
}
}
```

4. Trackers
You can see the tracker in:
'announce': 'http://bttracker.debian.org:6969/announce‘,
5. Check the trackers to see if the files are valid.
Trackers themselves should be verified by Verisgn or any other tool for tracker verification.

If the file is downloaded, keep it and post it here. If the torrent was incomplete or corrupted it might be possible to fix it with file recovery software.

Anonymous 12/10/2016 (Sat) 07:50:26 [Preview] No. 71 [X] del

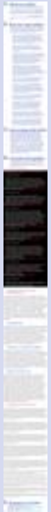
(5.22 KB 256x256 out.jpg)

- file header match (type: jpg) (block hash: 000000000000000001c49996dd0946a3eb734173fd2b0c66c84de64e96f835a5) (tx hash: 4b0cd7e191ef0a14a9b6ab1c5900be534118c20a332ff26407648168d2722a2e)

[redacted]

☐ Anonymous 12/10/2016 (Sat) 15:46:18 [Preview] No. 72 [X] del

(2.34 MB 720x8252 guide.png)



will be handy soon

☐ Anonymous 12/10/2016 (Sat) 15:55:24 [Preview] No. 73 [X] del

list used on the git code

```
if "D0CF11E0A1B11AE1".lower() in hexcode:
filetype += "DOC Header Found " # DOC Header
if "576F72642E446F63756D656E742E".lower() in hexcode:
filetype += "DOC Footer Found " # DOC Footer
if "D0CF11E0A1B11AE1".lower() in hexcode:
filetype += "XLS Header Found " # XLS Header
if "FEFFFFFF000000000000000057006F0072006B0062006F006F006B00".lower() in hexcode:
```

```
filetype += "XLS Footer Found " # XLS Footer
if "D0CF11E0A1B11AE1".lower() in hexcode:
filetype += "PPT Header Found " # PPT Header
if "A0461DF0".lower() in hexcode:
filetype += "PPT Footer Found " # PPT Footer
if "504B030414".lower() in hexcode:
filetype += "ZIP Header Found " # ZIP Header
if "504B050600".lower() in hexcode:
filetype += "ZIP Footer Found " # ZIP Footer
if "504B030414000100630000000000".lower() in hexcode:
filetype += "ZIPLock Footer Found " # ZLocked Encrypted
if "FFD8FFE000104A464946000101".lower() in hexcode:
filetype += "JPG Header Found " # JPG Header
if "474946383961".lower() in hexcode:
filetype += "GIF Header Found " # GIF Header
if "474946383761".lower() in hexcode:
filetype += "GIF Header Found " # GIF Header
if "2100003B00".lower() in hexcode:
filetype += "GIF Footer Found " # GIF Footer
if "25504446".lower() in hexcode:
filetype += "PDF Header Found " # PDF Header
if "2623323035".lower() in hexcode:
filetype += "PDF Header Found " # PDF Header
if "2525454F46".lower() in hexcode:
filetype += "PDF Footer Found " # PDF Footer
if "616E6E6F756E6365".lower() in hexcode:
filetype += "Torrent Header Found " # Torrent Header
if "1F8B".lower() in hexcode:
filetype += ".TAR.GZ Header Found " # TAR/GZ Header | Going to have lots of false positives
if "0011AF".lower() in hexcode:
filetype += "FLI Header Found " # FLI Header
if "504B03040A000200".lower() in hexcode:
filetype += "EPUB Header Found " # EPUB Header
if "89504E470D0A1A0A".lower() in hexcode:
filetype += "PNG Header Found " # PNG Header
if "6D51514E42".lower() in hexcode:
filetype += "8192PGP Header Found " # 8192 Header
if "6D51494E4246672F".lower() in hexcode:
filetype += "4096PGP Header Found " # 4096 Header
if "952e3e2e584b7a".lower in hexcode:
filetype += "2048PGP Header Found " # 2048 Header
if "526172211A0700".lower() in hexcode:
filetype += "Secret Header Found" # Secret Header
if "6D51454E424667".lower() in hexcode:
filetype += "RAR Header Found" # RAR Header
if "EFEDFACE".lower() in hexcode:
filetype += "UTF8 Header Found" # UTF8 header
if "4F676753".lower() in hexcode:
filetype += "OGG Header Found" # OGG Header
if "42494646".lower() in hexcode and "57415645".lower() in hexcode:
filetype += "WAV Header Found" # WAV Header
if "42494646".lower() in hexcode and "41564920".lower() in hexcode:
filetype += "AVI Header Found" # AVI Header
if "4D546864".lower() in hexcode:
filetype += "MIDI Header Found" # MIDI Header
if "377ABCAF271C".lower() in hexcode:
filetype += "7z Header Found" # 7z Header
if "0000001706".lower() in hexcode:
filetype += "7z Footer Found" # 7z Footer
```

☐ Anonymous 12/11/2016 (Sun) 00:49:04 [Preview] No. 74 [X] del

Logless BM bunker

http://gateway.glop.me/ipfs/QmSLGxufdzkNBMGqg1NwUuaCrcethPayN3jPzNYFtSDEkK/ffbbd7d918a09e876a06820498ec9e0c.jpg

Use the text in this image, generate its SHA256 hash value.
Add Chan -> Create a new chan -> chan name: [hash]

☐ Anonymous 12/12/2016 (Mon) 02:24:27 [Preview] No. 75 [X] del

https://zerobinqmdqd236y.onion.to/?7cd87b53ca199bdb#+Ht0Kg+aa8Nqx4oKXQIPM9UZibcVuZMMBMw22lc/+pw=

need to search each output script individually with trid that was sent TO the wikileaks address by some address, and in particular the time frame of 10/17 to 10/29

his dead man's switch was "check in by the end of the day on friday"

lowest number of transactions + highest fees + 0.0000000001 amounts paid (or close to 0 as possible because it is blackholed money since the data dictates the destination address and you don't have the priv key for the destination address)

and yes output scripts less than 40 are significant as well, because they do not un-hash (so to speak) to a valid address
also any output hex that is an ODD number is suspect

you can hide small shit, like keys or a text document inside a zip file (really small 2kb footprint)

the output script looks like this
"OP_DUP OP_HASH160 9f2fe1c79fefbc6166a906fc4fdadc61a08709fa OP_EQUALVERIFY OP_CHECKSIG"
if you take the hex string portion only:
9f2fe1c79fefbc6166a906fc4fdadc61a08709fa
and use it on this website:
http://bitcoinvalued.com/tools.php

put that string into the top right field. hit convert
Result: BitCoin address: 1FWhoQ3scrAPh7M7uy4jsk7VCNTe3vZeVL

This 9f2fe1 string is the hash160 of wallet 1FWhoQ3

Example: Looking at a transaction
"c234056fd6cc3bad6f51945e36893affc5493e824cfc3e90b51860a24f069a80"
you'll see that part of the transaction was sent to the wallet named:
"1FWhoQ3scrAPh7M7uy4jsk7VCNTe3vZeVL"
https://blockchain.info/tx/c234056fd6cc3bad6f51945e36893affc5493e824cfc3e90b51860a24f069a80

what has happened here is that the wallet 1FWhoQ3scrAPh7M7uy4jsk7VCNTe3vZeVL has received part of the UTXO (unspent transaction) from the sender

this transaction *proves* that

hell it was confirmed 20000 times or whatever

"27401 Confirmations"

so now the 1FWhoQ wallet may spend what they received - they are now able to spend it without throwing red flags

1FWhoQ has to put the right shit in the input scripts (bunch of version and shit and that's the input script and is basically automated by the wallet and cannot fuck up because it has to have the wallet's key to be able to spend the transaction out of the wallet)

and also 1FWhoQ will put the recipient's HASH160 into the output scripts

there will be one output script per recipient address

so if i wanted to send a file to the blockchain, i would have to send it to the addresses that my data dictates. because the data is in a particular order that creates the original file.

so if the first 20 bytes were ABCDABCDABCDABCDABCDABCD then it would send to this address: BitCoin address:
1NDUKKcNpLnAwcozASKSa11
and that is because 1NDUKK's hash160 value is ABCDABCDABCDABCDABCDABCD

if I don't own 1NDUKKcNpLnAwcozASKSa11, then I'm basically throwing money away because i can't send it out from the 1NDUKK wallet because i don't own that wallet because i don't have the private key and that is the most major part of the input script that allows the confirmations to occur(edited)

therefore the amount I send will be very, very small. but i may allow a big transaction fee (as a bounty) to make sure that transaction is confirmed and included in the blockchain quickly

and the way bitcoin works, when I send it, I have to send from only sources of unspent transactions. If I wanted to give you 1BTC and I had 10BTC, but I didn't have any unspent transaction in my wallet that was exactly 1BTC, then I'd have to send you chunks (for example 0.3 and 0.25 and 0.21 and 0.24) or i'd send you an amount larger than what i'm trying to send you if my smallest unspent transaction was one that i had received that was 2BTC. So my 10BTC wallet might be filled with four transactions -> 2BTC + 5BTC + 0.5BTC + 2.5BTC
and if i had to send you 2BTC, I'd want my 1BTC in change. so i have to include that as a recipient. i can choose to have it come back to my own wallet (if my wallet software allows and handles that properly) or i could give it another wallet that my wallet software auto

☐ Anonymous 12/12/2016 (Mon) 02:25:38 [Preview] No. 76 [X] del

need to search each output script individually with trid that was sent TO the wikileaks address by some address, and in particular the time frame of 10/17 to 10/29

his dead man's switch was "check in by the end of the day on friday"

lowest number of transactions + highest fees + 0.0000000001 amounts paid (or close to 0 as possible because it is blackholed money since the data dictates the destination address and you don't have the priv key for the destination address)

and yes output scripts less than 40 are significant as well, because they do not un-hash (so to speak) to a valid address
also any output hex that is an ODD number is suspect

you can hide small shit, like keys or a text document inside a zip file (really small 2kb footprint)

the output script looks like this
"OP_DUP OP_HASH160 9f2fe1c79fefbc6166a906fc4fdadc61a08709fa OP_EQUALVERIFY OP_CHECKSIG"
if you take the hex string portion only:
9f2fe1c79fefbc6166a906fc4fdadc61a08709fa
and use it on this website:
http://bitcoinvalued.com/tools.php

put that string into the top right field. hit convert
Result: BitCoin address: 1FWhoQ3scrAPh7M7uy4jsk7VCNTe3vZeVL

This 9f2fe1 string is the hash160 of wallet 1FWhoQ3

Example: Looking at a transaction
"c234056fd6cc3bad6f51945e36893affc5493e824cfc3e90b51860a24f069a80"
you'll see that part of the transaction was sent to the wallet named:
"1FWhoQ3scrAPh7M7uy4jsk7VCNTe3vZeVL"
https://blockchain.info/tx/c234056fd6cc3bad6f51945e36893affc5493e824cfc3e90b51860a24f069a80

what has happened here is that the wallet 1FWhoQ3scrAPh7M7uy4jsk7VCNTe3vZeVL has received part of the UTXO (unspent transaction) from the sender

this transaction *proves* that

hell it was confirmed 20000 times or whatever

"27401 Confirmations"

so now the 1FWhoQ wallet may spend what they received - they are now able to spend it without throwing red flags

1FWhoQ has to put the right shit in the input scripts (bunch of version and shit and that's the input script and is basically automated by the wallet and cannot fuck up because it has to have the wallet's key to be able to spend the transaction out of the wallet)

and also 1FWhoQ will put the recipient's HASH160 into the output scripts

there will be one output script per recipient address

so if i wanted to send a file to the blockchain, i would have to send it to the addresses that my data dictates. because the data is in a particular order that creates the original file.

so if the first 20 bytes were ABCDABCDABCDABCDABCDABCD then it would send to this address: BitCoin address: 1NDUKKcNpLnAwcozASKSa11
and that is because 1NDUKK's hash160 value is ABCDABCDABCDABCDABCDABCD

if I don't own 1NDUKKcNpLnAwcozASKSa11, then I'm basically throwing money away because i can't send it out from the 1NDUKK wallet because i don't own that wallet because i don't have the private key and that is the most major part of the input script that allows the confirmations to occur(edited)

therefore the amount I send will be very, very small. but i may allow a big transaction fee (as a bounty) to make sure that transaction is confirmed and included in the blockchain quickly

and the way bitcoin works, when I send it, I have to send from only sources of unspent transactions. If I wanted to give you 1BTC and I had 10BTC, but I didn't have any unspent transaction in my wallet that was exactly 1BTC, then I'd have to send you chunks (for example 0.3 and 0.25 and 0.21 and 0.24) or i'd send you an amount larger than what i'm trying to send you if my smallest unspent transaction was one that i had received that was 2BTC. So my 10BTC wallet might be filled with four transactions -> 2BTC + 5BTC + 0.5BTC + 2.5BTC
and if i had to send you 2BTC, I'd want my 1BTC in change. so i have to include that as a recipient. i can choose to have it come back to my own wallet (if my wallet software allows and handles that properly) or i could give it another wallet that my wallet software automatically generated

Transactions that have 911 in the value are significant because they are a

☐ **Anonymous** 12/12/2016 (Mon) 03:01:02 [Preview] No. 77

Just a note on something I thought was weird, could be totally unrelated:

Ed Snowden has mentioned zcash several times.

one article referencing it here: https://news.bitcoin.com/snowden-zcash-bitcoin-risks/

https://s6424n4x4bsmqs27.onion.to/POLAK/res/15.html